Lingua del documento :

ECLI:EU:C:2024:988

Provisional text

JUDGMENT OF THE COURT (Third Chamber)

28 November 2024 (*)

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data and the free movement of such data – Regulation (EU) 2016/679 – Data processed when drawing up a COVID-19 certificate – Data not collected from the data subject – Information to be provided – Exception to the obligation to provide information – Article 14(5)(c) – Data generated by the controller in the context of its own processes – Right to complain – Competence of the supervisory authority – Article 77(1) – Appropriate measures to protect the data subject's legitimate interests provided for by the Member State law to which the controller is subject – Measures relating to the security of data processing – Article 32)

In Case C169/23 [Másdi], (i)

REQUEST for a preliminary ruling under Article 267 TFEU from the Kúria (Supreme Court, Hungary), made by decision of 8 February 2023, received at the Court on 17 March 2023, in the proceedings

Nemzeti Adatvédelmi és Információszabadság Hatóság

v

UC,

THE COURT (Third Chamber),

composed of K. Jürimäe, President of the Second Chamber, acting as President of the Third Chamber, K. Lenaerts, President of the Court, acting as Judge of the Third Chamber, N. Jääskinen, M. Gavalec (Rapporteur) and N. Piçarra, Judges,

Advocate General: L. Medina,

Registrar: A. Calot Escobar,

having regard to the written procedure,

after considering the observations submitted on behalf of:

– the Nemzeti Adatvédelmi és Információszabadság Hatóság, by G.J. Dudás, ügyvéd,

– UC, by D. Karsai and V. Łuszcz, ügyvédek,

– the Hungarian Government, by Zs. Biró-Tóth and M.Z. Fehér, acting as Agents,

– the Czech Government, by L. Březinová, M. Smolek and J. Vláčil, acting as Agents,

– the European Commission, by A. Bouchagiar, C. Kovács and H. Kranenborg, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 6 June 2024,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 14(1) and (5)(c), Article 32 and Article 77(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; 'the GDPR').

2 The request has been made in proceedings between the Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information, Hungary) ('the national authority') and UC concerning the existence of an obligation to provide information on the part of the Budapest Főváros Kormányhivatala (Budapest Metropolitan Government Office, Hungary) ('the issuing authority'), which is responsible for issuing certificates of immunity to persons vaccinated against COVID-19 or having contracted that illness.

Legal context

European Union law

The GDPR

3 Under recitals 1, 10 and 61 to 63 of the GDPR:

'(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union … and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.

…

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. …

…

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. …

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. …'

4 Article 1 of that regulation, entitled 'Subject matter and objectives', provides, in paragraph 2:

'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.'

5 Article 4 of that regulation, entitled 'Definitions', states:

'For the purposes of this Regulation:

(1) "personal data" means any information relating to an identified or identifiable natural person ("data subject"); …

(2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

…

(7) "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; …

…'

6 Article 6 of the GDPR, entitled 'Lawfulness of processing', provides, in paragraph 1:

'Processing shall be lawful only if and to the extent that at least one of the following applies:

…

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

…

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

…'

7 Entitled ‘Processing of special categories of personal data’, Article 9 of that regulation provides, in paragraphs 1 and 2:

‘1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

…

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

…’

8 Chapter III of the GDPR, entitled ‘Rights of the data subject’ contains several sections, including Section 2, headed ‘Information and access to personal data’.

9 Section 2 of the GDPR includes Article 13 relating to ‘Information to be provided where personal data are collected from the data subject’, Article 14 relating to ‘Information to be provided where personal data have not been obtained from the data subject’, and Article 15 concerning the ‘Right of access by the data subject’.

10 Under Article 14 of that regulation:

‘1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller’s representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation …

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, …

…

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and in so far as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.'

11 Article 32 of the GDPR, entitled 'Security of processing', is worded as follows:

'1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.'

12 Article 55 of that regulation, entitled 'Competence', provides, in paragraph 1:

'Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.'

13 Article 57 of the GDPR, headed 'Tasks', provides, in paragraph 1:

'Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

…

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

…'

14 Article 58 of that regulation, entitled 'Powers', provides, in paragraph 3:

'Each supervisory authority shall have all of the following authorisation and advisory powers:

…

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

…'

15 Article 77 of that regulation, headed 'Right to lodge a complaint with a supervisory authority', provides, in paragraph 1:

'Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.'

16 Article 78 of the GDPR, entitled ‘Right to an effective judicial remedy against a supervisory authority’, is worded as follows:

‘1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.’

Regulation (EU) 2021/953

17 Article 10 of Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic (OJ 2021 L 211, p. 1), entitled ‘Protection of personal data’, provided, in paragraph 1:

‘[The GDPR] shall apply to the processing of personal data carried out when implementing this Regulation.’

Hungarian law

18 Under Paragraph 2(1) of the a koronavírus elleni védettségi igazolásról szóló 60/2021. (II.12.) Korm. rendelet (Government Decree No 60/2021 (II.12.) of 12 February on the certificate of immunity to coronavirus), in the version applicable to the dispute in the main proceedings (‘Decree No 60/2021’):

‘The immunity certificate shall contain:

(a) the name of the person concerned;

(b) the passport number of the person concerned, if he or she has a passport;

(c) the number of the permanent identity document of the person concerned, if he or she has a permanent identity document;

(d) the serial number of the immunity certificate;

(e) where proof of vaccination is provided, the date of vaccination;

(f) where proof of recovery from infection is provided, the date of validity of the certificate issued;

(g) a data storage code that is optically readable by computing devices, generated using the data listed in (a) to (f);

(h) the following wording in the form of text warnings:

(ha) “In order to be valid, the card must be shown in conjunction with an identity document or passport”

(hb) “Not transferrable”

(hc) “The rights associated with the certificate may be viewed on the website koronavirus.gov.hu”.’

19 In accordance with Paragraph 2(6) and (7) of Decree No 60/2021, the immunity certificate is to be issued by the issuing authority – either of its own motion or upon request – to any natural person entitled to receive it.

20 Paragraph 3(3) of that decree provides:

‘In the cases provided for in Paragraph 2(6)(c) and (d), the issuing authority shall collect, by the automated transmission of information – where necessary through the relevant departments of the Registry for the electronic organisation of identification data –,

(a) from the EESZT (Elektronikus Egészségügyi Szolgáltatási Tér (Electronic Healthcare Service Platform)) operator: the social security number of the data subject, the data set out in Paragraph 2(1)(e) and (g), and the data set out in subparagraph 1,

(b) from the body responsible for the recording of personal data and addresses: the name of the data subject, the number or identifier of his or her passport and permanent identity document, and his or her address.’

The dispute in the main proceedings and the questions referred for a preliminary ruling

21 An immunity certificate confirming the vaccination of UC, a natural person, against COVID-19 was issued by the issuing authority pursuant to Decree No 60/2021.

22 On 30 April 2021, UC launched an administrative procedure in relation to the processing of his personal data by lodging a complaint based on Article 77(1) of the GDPR with the national authority, seeking that the issuing authority be ordered to bring its processing operations in line with the provisions of the GDPR. In his complaint, the applicant claimed, inter alia, that the issuing authority had not drawn up and published any statement on the protection of personal data in relation to the issuing of immunity certificates and that there was no information concerning the purpose and legal basis of the processing of those data or the rights of data subjects and how those rights could be exercised.

23 In the procedure launched as a result of that complaint, the issuing authority declared that it performed its tasks linked to the issuing of immunity certificates on the basis of Article 2 of Decree No 60/2021, the processing of personal data having as a legal basis Article 6(1)(e) of the GDPR and Article 9(2)(i) of that regulation in so far as the processing of special categories of personal data is concerned.

24 In addition, the issuing authority stated that it obtained the personal data that it processed from another body, in accordance with the provisions of Decree No 60/2021. On that basis, it asserted that, pursuant to Article 14(5)(c) of the GDPR, it was not required to provide information on the processing of those data. It nonetheless drew up the requested statement concerning the protection of personal data and published it on its website.

25 By decision of 15 November 2021, the national authority rejected UC’s request and found that the issuing authority had no obligation to provide information because the processing of personal data in question was covered by the exception laid down in Article 14(5)(c) of the GDPR.

26 In particular, that authority took the view that Decree No 60/2021 formed the legal basis for that processing and that it expressly required the issuing authority to collect the data at issue. According to that authority, the publication of information on the processing of personal data by the issuing authority, on its website, amounted to good practice and not to a legal obligation.

27 Moreover, the national authority examined of its own motion whether there were any appropriate measures to protect the data subject's legitimate interests, within the meaning of the second part of Article 14(5)(c) of the GDPR, and it took the view that Articles 2, 3 and 5 to 7 of Decree No 60/2021 should be treated as such.

28 UC brought an administrative appeal against that decision before the Fővárosi Törvényszék (Budapest High Court, Hungary), which annulled the decision and ordered that authority to launch a new procedure.

29 In its judgment, that court considered that the exception laid down in Article 14(5)(c) of the GDPR was not applicable because certain personal data produced in relation to the immunity certificates were not collected from another body by the controller, but were generated by that controller itself in the performance of its tasks. That was the case, according to that court, so far as concerns the serial number of the immunity certificate, the expiry date of the certificate issued to a person who has contracted the illness, the QR code on the card, the barcode and other alphanumerical codes on the letter of delivery of the certificate and the personal data generated under the controller's file management processes. In that court's view, only personal data obtained from another body could be covered by the exception laid down in Article 14(5)(c) of the GDPR.

30 The national authority brought an extraordinary appeal against that judgment before the Kúria (Supreme Court, Hungary), the referring court.

31 It is in this context that the referring court seeks clarification, first of all, as to whether the exception laid down in Article 14(5)(c) of the GDPR can apply to all processing of personal data except processing which relates to personal data collected from the data subject.

32 In the affirmative, that court asks whether, in the context of a complaint procedure under Article 77(1) of the GDPR, the supervisory authority is competent to verify, with a view to ruling on the applicability of that exception, whether the controller's national law provides appropriate measures to protect the legitimate interests of the data subject.

33 Last, in the affirmative, the referring court wishes to know whether that verification also covers the appropriateness of the measures which the controller is required to implement, under Article 32 of the GDPR, in order to guarantee the security of the processing of personal data.

34 In those circumstances, the Kúria (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Must Article 14(5)(c) of [the GDPR], read in conjunction with Article 14(1) and recital 62 thereof, be interpreted as meaning that the exception laid down in Article 14(5)(c) does not [apply] to data generated by the controller [in the context of its own processes] but rather only to data which the controller has [specifically] obtained from another person?

(2) If Article 14(5)(c) of the GDPR is also applicable to data generated by the controller [in the context of its own processes], must the right to lodge a complaint with a supervisory authority, laid down in Article 77(1) of the GDPR, be interpreted as meaning that a natural person who alleges an infringement of the obligation to provide information is entitled, when exercising his or her right to lodge a complaint, to request an examination of whether Member State law provides appropriate measures to protect the data subject's legitimate interests, in accordance with Article 14(5)(c) of the GDPR?

(3) If the answer to the second question is in the affirmative, may Article 14(5)(c) of the GDPR be interpreted as meaning that the "appropriate measures" referred to in that provision require the national legislature to transpose (by means of legislation) the measures relating to the security of data laid down in Article 32 of the GDPR?'

35 On 16 January 2024, the Court asked the parties and the interested persons covered by Article 23 of the Statute of the Court of Justice of the European Union to answer certain questions in writing, pursuant to Article 61 of the Rules of Procedure of the Court of Justice. The applicant and the defendant in the main proceedings, the Hungarian and Czech Governments and the European Commission answered those questions.

Consideration of the questions referred

The first question

36 By its first question, the referring court asks, in essence, whether Article 14(5)(c) of the GDPR must be interpreted as meaning that the exception to the controller's obligation to provide information to the data subject, laid down in that provision, concerns only personal data which the controller collected from a person other than the data subject or whether it also concerns the personal data that that controller generated itself in the performance of its tasks.

37 Article 14(1), (2) and (4) of that regulation specifies the information which the controller must provide to the data subject, within the meaning of Article 4(1) of that regulation, where personal data have not been obtained from the data subject.

38 Article 14(5) of that regulation sets out exceptions to that obligation. Among those exceptions, subparagraph (c) of Article 14(5) provides that that obligation does not apply where and in so far as obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests.

39 In order to determine whether that exception covers personal data generated by the controller itself – in the performance of its tasks – from data obtained from a person other than the data subject, it is necessary, in accordance with settled case-law, to consider not only the wording of the provision laying down that exception but also its context and the objectives pursued by the legislation of which it forms part (see, to that effect, judgment of 12 January 2023, *Nemzeti Adatvédelmi és Információszabadság Hatóság*, C132/21, EU:C:2023:2, paragraph 32 and the case-law cited).

40 In the first place, the subject matter of the 'obtaining or disclosure', referred to in Article 14(5)(c) of the GDPR, must be determined in the light of the wording of that provision.

41 Indeed, first, there is a discrepancy between the different language versions of that provision. The French language version of that provision refers to obtaining or disclosing 'information' while, first of all, the Hungarian ('adat'), Estonian ('isikuandmed'), Croatian ('podataka'), Lithuanian ('duomenų'), Dutch ('gegevens'), Portuguese ('dados'), Romanian ('datelor') and Swedish ('uppgifter') language versions refer to obtaining or disclosing 'data', next, the Finnish language version includes a term ('tietojen') which can cover both 'data' and 'information' and, finally, the Bulgarian, Spanish, Czech, Danish, German, Greek, English, Italian, Latvian, Maltese, Polish, Slovak and Slovenian versions do not refer to the subject matter of that obtaining or disclosure.

42 In accordance with further settled case-law, the wording used in one language version of a provision of EU law cannot serve as the sole basis for the interpretation of that provision, or be made to override the other language versions. Provisions of EU law must be interpreted and applied uniformly in the light of the versions existing in all languages of the European Union. Where there is a divergence between the various language versions of an EU legislative text, the provision in question must be interpreted by reference to the general scheme and purpose of the rules of which it forms part (judgment of 21 March 2024, *Cobult*, C76/23, EU:C:2024:253, paragraph 25 and the case-law cited).

43 As regards the general scheme of the GDPR, Article 14(5) of that regulation must be read in the light of recitals 61 and 62 thereof, which refer to (i) 'the personal data … obtained [and the] personal data … disclosed' as well as 'the recording or disclosure of the personal data … expressly laid down by law' and (ii) 'information … given' or to be 'provided'. The interpretation according to which 'obtaining or disclosure', within the meaning of Article 14(5)(c) of the GDPR, concerns personal data is moreover confirmed by the wide scope of the concept of 'processing', within the meaning of Article 4(2) of the GDPR, which covers any operation performed on personal data (see, to that effect, judgment of 5 October 2023, *Ministerstvo zdravotnictví (COVID-19 mobile application)*, C659/22, EU:C:2023:745, paragraph 27 and the case-law cited).

44 As regards the purpose of the rules of which Article 14(5)(c) of the GDPR forms part, it is sufficient to observe, as the Advocate General did in point 31 of her Opinion, that the *ratio legis* of that exception is that the obligation to provide information to the data subject imposed by Article 14(1), (2) and (4) of that regulation is not justified when another provision of EU law or of Member State law imposes on the controller a sufficiently comprehensive and binding obligation to provide to the data subject information relating to obtaining or disclosure of personal data. In the situation covered by Article 14(5)(c), data subjects must have sufficient knowledge of the detailed rules and the purposes of obtaining or disclosing those data.

45 Consequently, it must be considered that, in the light of the wording of all the language versions of Article 14(5)(c) of the GDPR, that provision must be understood as referring to obtaining or disclosure of personal data.

46 Second, it must be noted that the wording of Article 14(5)(c) of the GDPR does not limit the exception which it lays down merely to personal data obtained by the controller from a person other than the data subject, nor does it exclude data generated by the controller itself, in the performance of its tasks, from such data.

47 It follows that personal data which were 'obtained', within the meaning of that provision, by the controller are all those data which that controller collects from a person other than the data subject and those which that controller generated itself, in the performance of its tasks, from data obtained from a person other than the data subject.

48 In the second place, it must be observed that the material scope of Article 14 of the GDPR is defined negatively by reference to Article 13 of that regulation. As is apparent from those provisions' headings themselves, Article 13 concerns the information to be provided where personal data are collected from the data subject, while Article 14 concerns the information which must be provided where personal data have not been collected from the data subject. In the light of that dichotomy, all situations in which data are not collected from the data subject fall within the material scope of Article 14.

49 Therefore, it follows from the combined interpretation of Articles 13 and 14 of the GDPR that both personal data obtained by the controller from a person other than the data subject, and data generated by the controller itself – which, on account of their nature, have also not been obtained from the data subject – fall within the scope of Article 14. It follows that the exception laid down in Article 14(5)(c) covers both categories of data.

50 In the third place, Article 14(5)(c) of the GDPR must be interpreted in a way which is consistent with the objective pursued by that regulation, which consists, inter alia, as is apparent from Article 1 thereof, read in the light of recitals 1 and 10 thereof, in ensuring a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, as enshrined in Article 8(1) of the Charter of Fundamental Rights and Article 16(1) TFEU (see,

to that effect, judgment of 7 March 2024, *IAB Europe*, C604/22, EU:C:2024:214, paragraph 53 and the case-law cited).

51 In that regard, it is apparent from recital 63 of the GDPR that the EU legislature intended a data subject, within the meaning of that regulation, to have the right of access to personal data which have been collected concerning him or her, in order to be aware of, and verify, the lawfulness of the processing.

52 Accordingly, the controller may be exempted from its usual obligation to provide information to a data subject provided that that data subject is able to exercise control over those personal data and exercise the rights conferred upon him or her by the GDPR.

53 In accordance with the objective pursued by that regulation, the exception to the obligation to provide information to the data subject, laid down in Article 14(5)(c) of the GDPR, requires that, first, the obtaining or disclosure of personal data by the controller be expressly laid down by Union or Member State law to which that controller is subject. Second, that right must provide appropriate measures to protect the data subject's legitimate interests.

54 It follows that, in order to be fully consistent with the objective pursued by the GDPR, the application of Article 14(5)(c) of that regulation is subject to strict compliance with the conditions that that provision lays down, that is to say, inter alia, the existence of a level of protection of the data subject at least equivalent to that guaranteed by Article 14(1) to (4) of that regulation.

55 Having regard to the foregoing considerations, the answer to the first question is that Article 14(5)(c) of the GDPR must be interpreted as meaning that the exception to the controller's obligation to provide information to the data subject, laid down in that provision, concerns all personal data, without distinction, that have not been collected by the controller directly from the data subject, whether those data have been obtained by the controller from a person other than the data subject or whether they have been generated by the controller itself, in the performance of its tasks.

The second and third questions

56 By its second and third questions, which should be examined together, the referring court asks, in essence, whether Article 14(5)(c) and Article 77(1) of the GDPR must be interpreted as meaning that, in a complaint procedure, the supervisory authority is competent to verify whether the Member State law to which the controller is subject provides appropriate measures to protect the data subject's legitimate interests, for the purposes of the application of the exception laid down in Article 14(5)(c) and, in the affirmative, whether that verification also covers the appropriateness of the measures which the controller is required to implement, under Article 32 of that regulation, in order to guarantee the security of the processing of personal data.

57 In the first place, it must be borne in mind that, according to Article 77(1) of the GDPR, without prejudice to any other administrative or judicial remedy, every data subject has the right to lodge a complaint with a supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes that regulation.

58 As regards the competence of the supervisory authorities, Article 55(1) of that regulation provides that each supervisory authority is competent, on the territory of its own Member State, for the performance of the tasks assigned to it and the exercise of the powers conferred on it in accordance with that regulation.

59 So far as concerns those tasks, Article 57(1)(a) of the GDPR provides that each supervisory authority must monitor and enforce the application of that regulation on its territory.

60 The GDPR does not include any provision such as to exclude certain aspects of the application of the exception laid down in Article 14(5)(c) of that regulation from the competence of those supervisory authorities.

61 Under that provision, the controller is exempted from the obligation to provide to a data subject the information set out in Article 14(1), (2) and (4) of the GDPR where and in so far as, first, obtaining or disclosure of personal data is expressly laid down by Union or Member State law to which the controller is subject and, second, that law provides appropriate measures to protect the data subject's legitimate interests.

62 Therefore, a complaint under Article 77(1) of the GDPR may be based on an infringement of the controller's obligation to provide information, alleging non-compliance with the conditions for the application of the exception laid down in Article 14(5)(c) of that regulation.

63 As regards the first condition, recalled in paragraph 61 of the present judgment, the supervisory authority before which such a complaint is brought may be required to verify whether Union law or national law provides that the controller must obtain or disclose personal data.

64 As regards the second condition, it must be noted, as the Advocate General observed in points 67 and 69 of her Opinion, that the scope of the expression 'appropriate measures to protect the data subject's legitimate interests' is not defined in the GDPR. That said, the provisions of EU or Member State law which provide for such measures and to which the controller is subject must guarantee, as noted in paragraph 54 of the present judgment, a level of protection of the data subject with regard to the processing of his or her personal data which is at least equivalent to that provided for in Article 14(1) to (4) of that regulation. Thus, those provisions must be such as to put the data subject in a position to enable him or her to exercise control over his or her personal data and to exercise the rights conferred on him or her by the GDPR.

65 To that end, it is important, in particular, that those provisions state, in a clear and foreseeable manner, the source from which the data subject will obtain information about the processing of his or her personal data.

66 In the context of the transmission of personal data between bodies of a Member State and the generation of such data by a controller from the data collected from a person other than the data subject, it should be noted that, in the event of a complaint by that data subject, it will be for the supervisory authority to verify, inter alia, whether the relevant national or EU law defines with sufficient precision the various types of personal data to be obtained or disclosed, as well as the personal data that it is required to generate in the performance of its duties, and whether that law sets out the manner in which the data subject actually has access to the information referred to in Article 14(1), (2) and (4) of the GDPR.

67 As the Commission notes in its written observations, the verification, by a supervisory authority, of whether all the conditions for the application of the exception laid down in Article 14(5)(c) of the GDPR are satisfied does not, however, fall within the scope of an examination of the validity of the relevant provisions of national law. That authority takes a decision only on whether or not, in a given case, the controller is entitled to rely on the exception laid down in that provision in relation to the data subject.

68 As regards the outcome of such a verification, it should be recalled that, under Article 78 of that regulation, where, in a given case, the supervisory authority decides that the data subject's complaint is unfounded, the data subject must have, in his or her Member State, the right to an effective judicial remedy against that rejection decision.

69 By contrast, where that authority takes the view that the complaint is well founded and that the conditions for applying the exception laid down in Article 14(5)(c) of that regulation are not met, it is to

order the controller to provide the information to the data subject, in accordance with Article 14(1), (2)and (4) of that regulation.

70 In the second place, as regards whether that verification must also cover the appropriateness, in the light of Article 32 of the GDPR, of the measures which the controller is required to implement in order to ensure the security of processing, it must be pointed out that Article 14(5)(c) of that regulation establishes an exception only to the obligation to provide information laid down in Article 14(1), (2) and (4) of that regulation, without providing for a derogation from the obligations contained in other provisions of that regulation, including Article 32 thereof.

71 Article 32 obliges the controller and any processor of that controller to implement appropriate technical and organisational measures to ensure an adequate level of security for the processing of personal data. The appropriateness of such measures must be assessed in a concrete manner, by taking into account the risks associated with the processing concerned and by assessing whether the nature, content and implementation of those measures are appropriate to those risks (see, to that effect, judgments of 14 December 2023, *Natsionalna agentsia za prihodite*, C340/21, EU:C:2023:986, paragraphs 42, 46 and 47, and of 25 January 2024, *MediaMarktSaturn*, C687/21, EU:C:2024:72, paragraphs 37 and 38).

72 In the light of the respective wording of those two provisions, it should be noted that the obligations enshrined in Article 32 of the GDPR, which must be complied with in all circumstances and irrespective of whether or not there is an obligation to provide information under Article 14 of that regulation, differ in nature and scope from the obligation to provide information laid down in Article 14 of that regulation.

73 Thus, in the event of a complaint under Article 77(1) of the GDPR, on the ground that the controller wrongly relied on the exception laid down in Article 14(5)(c) of that regulation, the subject matter of the verifications to be carried out by the supervisory authority is delimited by the scope of Article 14 of that regulation alone, since compliance with Article 32 thereof is not included in those verifications.

74 Having regard to the foregoing considerations, the answer to the second and third questions is that Article 14(5)(c) and Article 77(1) of the GDPR must be interpreted as meaning that, in a complaint procedure, the supervisory authority is competent to verify whether the Member State law to which the controller is subject provides appropriate measures to protect the data subject's legitimate interests, for the purposes of the application of the exception laid down in Article 14(5)(c). That verification does not however cover the appropriateness of the measures which the controller is required to implement, under Article 32 of that regulation, in order to guarantee the security of processing of personal data.

Costs

75 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Third Chamber) hereby rules:

1. **Article 14(5)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**

must be interpreted as meaning that the exception to the controller's obligation to provide information to the data subject, laid down in that provision, concerns all personal data, without distinction, that have not been collected by the controller directly from the data subject, whether those data have been

obtained by the controller from a person other than the data subject or whether they have been generated by the controller itself, in the performance of its tasks.

2. **Article 14(5)(c) and Article 77(1) of Regulation 2016/679**

must be interpreted as meaning that, in a complaint procedure, the supervisory authority is competent to verify whether the Member State law to which the controller is subject provides appropriate measures to protect the data subject's legitimate interests, for the purposes of the application of the exception laid down in Article 14(5)(c). That verification does not however cover the appropriateness of the measures which the controller is required to implement, under Article 32 of that regulation, in order to guarantee the security of processing of personal data.

[Signatures]

* Language of the case: Hungarian.

i The name of the present case is a fictitious name. It does not correspond to the real name of any of the parties to the proceedings.